

Appln. No.: 09/819,509  
Amendment October 18, 2005  
Reply to Office Action of July 25, 2005

PATENT

**Remarks/Arguments:**

**Status of Claims**

Claims 1-20 are pending and stand rejected.

By this Amendment, a minor change is made to claim 6 and new claims 21 and 22 are added.

Applicants contend that no new matter has been added by the new claims, and accordingly, entry and approval of same is proper and respectfully requested. Support for the new claims are found throughout the specification, and, more particularly, in the specification, for example, at paragraph [0023].

**Rejection of Claims 1-20 Under 35 U.S.C. § 103(a)**

In the Office Action at page 2, claims 1-20 stand rejected under 35 U.S.C. §103(a) as being obvious over the combination of Leslie Lamport (hereinafter referred to as Lamport) entitled "Password Authentication with Insecure Communication," in view of Brown et al. (U.S. Patent No. 6,618,806) (hereinafter referred to as Brown).

Applicants respectfully traverse this rejection and request reconsideration.

**Claim 1**

Claim 1 is directed to a method of forming a strong password, and recites "combining the biometric data and the one-time password to form the strong password."

**Lamport Reference**

The Examiner acknowledges on page 3 of the Action that the Lamport reference does not teach "a mechanism that obtains biometric data from a user combining the biometric data and the one-time password to form a strong password."

It is submitted based on this acknowledgement that Lamport does not teach or suggest the above mentioned recitation of claim 1.

**Brown Reference**

The Examiner contends, on page 3 of the Action, that Brown teaches "a biometric user authentication method and system wherein biometric data is obtained and is combined with a password to authenticate a user (See Column 3, lines 21-25, 51-57 [of Brown])."

Applicants respectfully disagree with the Examiner because in Brown biometric data is not combined with anything. Brown discloses a system and method for biometric user

Appl. No.: 09/819,509  
Amendment October 18, 2005  
Reply to Office Action of July 25, 2005

PATENT

authentication. In the Brown system, "[a]t authentication time, the primary biometric type and technology are compared with the client workstation's capabilities. If the workstation does not have the necessary resources to capture the primary biometric, the user can be optionally challenged for a password." (See Brown et al. at column 4, lines 20-24.) That is, Brown discloses a method which uses biometrics to authenticate a user and in the absence of the appropriate biometrics uses passwords for such authentication.

Brown is silent regarding combining biometric data and a password to form a strong password, as required by claim 1, and, more particularly, regarding combining biometric data and a one-time password.

Accordingly, claim 1 is not subject to this rejection under 35 U.S.C. §103(a) and is submitted to be allowable over Lamport in view of Brown for the reasons set forth above.

#### **Claims 3, 16 and 18**

Claims 3, 16 and 18 are submitted to be patentable for at least similar reasons to those of claim 1. For example, claim 3 is submitted to be patentable for at least the recites that the strong password includes "one-time password and biometric data from a user."

#### **Claims 2, 4-5, 17 and 19-20**

Claims 2, 4-5, 17 and 19-20 include all of the features of their respective independent claims from which they ultimately depend. Thus, Applicant contends that these claims are also allowable for at least the reasons set forth above.

#### **Claim 6**

Claim 6 is directed to a system for implementing secure access to a remote computer, and recites "at least one first computer securely coupled to the remote computer system; at least one second computer coupled to said at least one first computer and configured to obtain identifying information from a user; wherein the second computer passes the identifying information to the first computer, the first computer passes the identifying information to the remote computer system and the remote computer system verifies the identifying information."

#### **Lamport Reference**

Lamport discloses at page 771, second column the use of a microcomputer in the user's terminal. Lamport is silent regarding a remote computer and first and second computers, as required by claim 6.

Appl. No.: 09/819,509  
Amendment October 18, 2005  
Reply to Office Action of July 25, 2005

PATENT

### **Brown Reference**

Brown discloses, at the portions cited by the Examiner, that FIG. 1 illustrates an HA-API with two interfaces. A first Interface is an application API 101 and a second interface is a Biometric Service Provider (BSP) Interface 111. Nothing in this disclosure teaches or suggests a remote computer and first and second computers interacting with each other (i.e., the second computer passing Identifying Information to the first computer, the first computer passing the Identifying information to the remote computer system and the remote computer system verifying the Identifying information," as required by claim 6. Brown does disclose at column 5, lines 25-29 that "If the verification server 222 verifies that the user is authorized to log on, the server will retrieve the user's password from the database 221 and send the user's password back to the workstation where the log-on will be completed." This passage, however, discloses only the server and the workstation. The subject invention, as defined by claim 6 requires three computers: a remote computer, a first computer and a second computer. Thus, Brown does not provide the material that is missing from Lamport. Accordingly, claim 6 is not subject to this rejection under 35 U.S.C. §103(a) and is submitted to be allowable over Lamport in view of Brown for the reasons set forth above.

### **Claim 12**

Claim 12 is submitted to be patentable for at least similar reasons to those of claim 6.

### **Claims 7-11 and 13-15**

Claims 7-11 and 13-15 include all of the features of their respective independent claims from which they ultimately depend. Thus, Applicant contends that these claims are also allowable for at least the reasons set forth above.

### **New Claims 21 and 22**

New claims 21 and 22 include recitations of "concatenating the biometric data with the one-time password to form the strong password" and "combining the biometric data with the one-time password using one or more arithmetic operations with a result used as the strong password," respectively. It is submitted that claims 21 and 22 are patentable for the same reasons as claim 1, and separately patentable for these respective recitations.

Appln. No.: 09/819,509  
Amendment October 18, 2005  
Reply to Office Action of July 25, 2005

PATENT

**CONCLUSION**

In view of the above, it is submitted that claims 1 to 22 are in condition for allowance and early notification to that effect is earnestly solicited.

Respectfully submitted,



Kenneth N. Nigon, Reg. No., 31,549  
Eric Berkowitz, Reg. No., 44,030  
Attorneys for Applicant

KNN/EB/ks

Dated: October 18, 2005

P.O. Box 980  
Valley Forge, PA 19482  
(610) 407-0700

The Commissioner for Patents is hereby authorized to charge payment to Deposit Account No. 18-0350 of any fees associated with this communication.

I hereby certify that this correspondence is being deposited with the United States Postal Service as first class mail, with sufficient postage, in an envelope addressed to: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450 on: October 18, 2005

  
Kathleen Spina

K:\PAT\202US\OA 7.25.05\AMENDMENT10.2005.DOC